

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Shapiro, Eileen et al. Docket No.: 1525B/116
Appl. No.: 10/786,355 Art Unit: 2435
Filing Date: February 25, 2004 Examiner: Debnath, Suman
Confirmation: Date: January 10, 2011
Invention: SYSTEM AND METHOD FOR PROVIDING ACCESS TO
VERIFIED PERSONAL BACKGROUND DATA

VIA USPTO ELECTRONIC FILING SYSTEM

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

The Applicants submit this Appeal Brief after filing a Notice of Appeal on November 9, 2010 in response to the

Table of Contents

<i>Table of Contents</i>	2
<i>Real Party in Interest</i>	3
<i>Related Appeals and Interferences</i>	4
<i>Status of Claims</i>	5
<i>Status of Amendments</i>	6
<i>Summary of Claimed Subject Matter</i>	7
<i>Grounds of Rejection to be Reviewed on Appeal</i>	10
<i>Argument</i>	11
I. The Office's combination of Walker, Ballantyne, and Bisbee fails to meet all of the limitations of the claims, and in particular, fails to teach the logical flow claimed with respect to the use of the candidate identifier.	11
II. As a matter of law, the combination of Walker with a reference that breaks Walker's anonymity renders Walker inoperative for its intended purpose.	14
<i>Appendix I: Claims Appendix</i>	17
<i>Appendix II: Evidence Appendix</i>	22
<i>Appendix III: Related Proceedings Appendix</i>	23

Real Party in Interest

The real party in interest is VeriVita LLC, the assignee of record, which is managed by The Hillcrest Group, Inc. of Cambridge, MA.

Related Appeals and Interferences

Appellants' legal representative is not aware of any other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on, the Board's decision in the present appeal.

Status of Claims

Claims 1-16 are pending in the application. Claims 17-56 stand canceled. The present appeal is taken with respect to all pending claims 1-16.

Status of Amendments

On August 16, 2010, the Appellants filed a response to the final rejection dated May 14, 2010. The August 16 response included no amendments to the claims, only remarks clarifying the Appellants' position. As understood by Appellants, the response was entered into the record by the Examiner in the Advisory Action dated September 16, 2010.

Summary of Claimed Subject Matter

The claimed subject matter enables a job candidate to control the communication of his verified background information to prospective employers of the candidate's choosing, in a way that assures those employers of the veracity of that information. The claimed subject matter achieves this result by establishing logical flow of a token (namely, the claimed "candidate identifier") between the various parties in a specific manner that is defined by the claims herein.

Claim 1 defines logical flow of the candidate identifier in a manner summarized below, where we also make reference to the limitations of claim 1.¹ Claim 1 requires that the candidate identifier is:

- established in a storage medium (claim 1, limitation a);
- then communicated to the candidate (claim 1, limitation b);
- next received by the outside user directly or indirectly from the candidate (claim 1, limitation c); and finally
- received from the outside user (claim 1, limitation c) as a condition of distributing an electronic document to the outside user (claim 1, limitation d).

This sequence of steps achieves the desired result because, while the candidate has control over the recipient of his background information, he does not have control over the information that verifies it.

Independent claim 1 provides a method of providing access to a candidate's personal background data, wherein the data have been verified. (Page 4, line 19 – page 6, line 8.) The method has two logical phases that occur at different times. (Fig. 1, the first phase includes elements 11 and 12, the second phase includes element 13, and the data themselves include element 14.)

The first logical phase includes establishing a data record relating to the candidate's personal background data, in a digital storage medium, the data record having a candidate identifier that identifies the candidate and including a set of components

¹ Claim 16, directed to a system that is analogous to the method of claim 1, has similar limitations.

based on information supplied by the candidate, each component being potentially verifiable. (Page 4, line 19 – page 5, line 9; also Figs. 4A-4B, elements 405, 408, 411, 413, and 416 and page 8, line 26 – page 9, line 24). The data record also has a corresponding set of query results obtained at a first time, the corresponding set including, with respect to each component, the result of a verification query to a third party. (Page 5, lines 10-18; also Figs. 5A-5B, elements 503, 506, 508-510, and 512 and page 9, line 25 – page 11, line 7.) The first phase also includes communicating the candidate identifier to the candidate. (Fig. 1, element 12 and page 5, line 27 – page 6, line 8.)

The second logical phase includes receiving, after the first time, over a communication network, the candidate identifier from an outside user wanting verification of the candidate's personal background data. (Fig. 7A, element 701 and page 12, lines 24 – 28; also Fig. 3, element 32 and page 7, line 5 – page 8, line 19.) The outside user received the candidate identifier directly or indirectly from the candidate. (Page 5, line 27 – page 6, line 8.) The second logical phase concludes with distributing, to the outside user, over the communication network, in response to receiving the candidate identifier, an electronic document (page 9, line 25 – page 10, line 1) including the data record and an electronic authentication of the contents of the data record, the electronic authentication capable of revealing unauthorized modifications of the contents of the data record. (Figs. 6A-6B, elements 604, 607, and 611 and page 11, line 8 – page 12, line 23.)

Independent claim 16 provides a system for providing access to a candidate's personal background data, wherein the data have been verified. (Fig. 3, elements 33 and 34.) The system includes a storage arrangement on which is stored a database having a plurality of data records, each data record relating to personal background data of a candidate. (Fig. 3, element 33 and page 7, line 17 – page 8, line 2.) Each data record has a candidate identifier that identifies the candidate and that is communicated to the candidate. (Page 4, lines 19-24; also Fig. 1, element 12 and page 5, line 27 – page 6, line 8.) Each data record includes a set of components based on information supplied by a candidate, each component being potentially verifiable. (Page 4, line 19 – page 5, line 9; also Figs. 4A-4B, elements 405, 408, 411, 413, and 416 and page 8, line 26 – page 9, line

24). Each data record also has a corresponding set of query results obtained at a first time, the corresponding set including, with respect to each component, the result of a verification query to a third party. (Page 5, lines 10-18; also Figs. 5A-5B, elements 503, 506, 508-510, and 512 and page 9, line 25 – page 11, line 7.)

The system also includes a process (Fig. 1, element 13 and page 8, lines 3-15), running on a computer in communication with the storage arrangement (Fig. 2, element 34), for selectively distributing, to an authorized person presenting an identifier received directly or indirectly from the candidate (page 5, line 27 – page 6, line 8; also Fig. 2, element 38 and page 8, lines 3-15), in response to receiving the identifier after the first time, over a communication network (Fig. 2, element 32), an electronic document (page 9, line 25 – page 10, line 1) including the candidate's data record and an electronic authentication of the contents of the data record, the electronic authentication capable of revealing unauthorized modifications of the contents of the data record. (Figs. 6A-6B, elements 604, 607, and 611 and page 11, line 8 – page 12, line 23.)

Grounds of Rejection to be Reviewed on Appeal

Whether claims 1-16 are unpatentable under 35 U.S.C. 103(a) over the combination of U.S. 5,884,270 (Walker) in view of U.S. 5,867,821 (Ballantyne) and U.S. 5,748,738 (Bisbee).

Argument

I. The Office’s combination of Walker, Ballantyne, and Bisbee fails to meet all of the limitations of the claims, and in particular, fails to teach the logical flow claimed with respect to the use of the candidate identifier.

To establish a *prima facie* case of obviousness based on a combination of references, “all words in a claim must be considered in judging the patentability of that claim against the prior art.” *In re Wilson*, 424 F.2d 1382 (CCPA 1970); MPEP § 2143.03. Because the combination urged in the rejection fails to meet all claim limitations, as explained below, the office action fails to set forth a *prima facie* basis for rejection of the claims.

As a preliminary matter, the Examiner correctly notes that Walker fails to disclose a candidate identifier that identifies the candidate. Office Action, p. 3 (May 14, 2010). To fill this gap left by Walker, the Office argues that Ballantyne teaches the claimed candidate identifier. The Office cites col. 8, lines 17-29 of Ballantyne, which state in part that a “unique identification number (ID) is assigned to each user and their personal profile data is stored electronically online.”

However, the ID of Ballantyne simply does not have the logical flow required by the claims. As described above with respect claims 1 and 16, the candidate identifier is:

- established in a storage medium (claim 1, limitation a);
- then communicated to the candidate (claim 1, limitation b);
- next received by the outside user directly or indirectly from the candidate (claim 1, limitation c); and finally
- received from the outside user (claim 1, limitation c) as a condition of distributing an electronic document to the outside user (claim 1, limitation d).

Thus the candidate identifier is communicated three times: to the candidate, to the outside user, then back to the system implementing the method. In Ballantyne, once the ID is issued to the medical professional, the medical professional uses the ID to access patient records. Ballantyne, lines 28-30. But that is the end of the flow as far as Ballantyne’s identifier is concerned. There is no suggestion that the recipient of an identifier (i.e., the

claimed candidate) passes it to a third party to enable the third party to access information about the first recipient, or that the third party passes the identifier back to the implementing system, as required by the claims. In short, the second and third legs of the triangle are missing from Ballantyne.

In fact, Ballantyne teaches away from the claim requirement of passing an identifier to an outside user, because Ballantyne requires that any person attempting to use the identifier be authenticated using queries such as the medical professional's mother's maiden name, information that would not be available to an outside user. Ballantyne, col. 8, lines 33-38. Ballantyne thus teaches away from limitations (b) and (c) of claim 1, and the corresponding limitations of claim 16.

Ballantyne is inapposite for another reason. The claims require that the candidate identifier gates access to the candidate's own verified information. Assuming for the moment that Ballantyne has any relevance whatsoever to the claimed subject matter, Ballantyne's disclosed ID gates access by the medical professional to the patient's verified information, not that of the medical professional. Ballantyne, col. 8, lines 41-43. Ballantyne's identifier is thus being used for the wrong purpose.

The Examiner also admits that Walker and Ballantyne fail to disclose limitations (c) or (d) of claim 1, or their counterparts in claim 16, and cites Bisbee as meeting these limitations. Office Action, pp. 4, 8. However, Bisbee also fails to teach the claimed candidate identifier lifecycle. Bisbee teaches electronic signatures (Bisbee, title), but says nothing about identifiers, let alone using an identifier in the manner required by the claims as recited above.

The Office cited passages in Bisbee, on page 4 of the Office Action, that supposedly read on the candidate identifier lifecycle requirements "receiving... the candidate identifier" (claim 1, limitation (c)) and "distributing... in response to receiving the candidate identifier" (claim 1, limitation (d)). However, these passages fail to mention either candidates or identifiers. Instead, these passages discuss a method and apparatus for authenticating an electronic document, and are not directed to the claim limitations pertaining to the candidate identifier at all. Moreover, it is not immediately

clear from the Office Action what disclosure in Bisbee is meant to play the role of the candidate identifier, despite the Office’s blanket assertion that such an identifier is present. Nevertheless, the attorney for the Appellant has carefully read Bisbee in an attempt to locate the candidate identifier to which the Office is alluding. The words “candidate” and “identifier” are nowhere to be found in this reference. The closest disclosure that was located occurs in the paragraph beginning in col. 4, line 61, which discusses “personal identification information such as the recipient’s biometric information... or a PIN.” But this information is not the claimed candidate identifier—it is not received from an outside user wanting verification of the candidate’s personal background data, the outside user having received the candidate identifier directly or indirectly from the candidate. Biometric information and a personal identification number respectively pertain to the individual’s physical characteristics and knowledge, not her background, and thus cannot be the claimed “background information.”

Indeed, and in addition, since claim 1, limitation (c) requires that the outside user has “received the candidate identifier directly or indirectly from the candidate” and since none of the offered references disclose communicating the identifier to the candidate in first place, it cannot possibly be the case that the outside user has “received the candidate identifier directly or indirectly from the candidate.” These passages therefore fail to disclose or suggest these claim limitations, which the Examiner has already admitted are not found in the other cited art. See Office Action, p. 4.

The Office has therefore failed to establish a *prima facie* case of obviousness, because it has failed to account for all of the claim limitations, and in particular has failed to account for at least three limitations. The cited art fails to disclose or suggest, alone or in combination, a candidate identifier that is first established, then communicated to the candidate, received by the outside user directly or indirectly from the candidate, and finally received from the outside user, as claimed. The cited prior art also fails to disclose or suggest receiving a candidate identifier from an outside user wanting verification of the candidate’s personal background data, the outside user having received the claimed candidate identifier. Finally, the cited prior art fails to disclose or suggest distributing an electronic document to the outside user in response to receiving the

candidate identifier, as claimed, because the cited prior art does not teach the second or third legs of the candidate identifier lifecycle. For at least these reasons, claims 1-16 are not obvious in view of this combination.

II. As a matter of law, the combination of Walker with a reference that breaks Walker's anonymity renders Walker inoperative for its intended purpose.

In making a rejection under 35 U.S.C. § 103(a), obviousness can be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation do to so. However, as a matter of law, there is no suggestion or motivation to make a proposed modification if it would render the prior art invention being modified unsatisfactory for its intended purpose.

MPEP 2143.01(V); *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). This is precisely the kind of modification that the Office has made here: the proposed modification of Walker using Ballantyne (or Bisbee) undermines Walker's expressly stated purpose.

Walker is directed to a method and system for facilitating anonymous communications. Walker, title and abstract. Walker's intended purpose is to provide a system that allows for electronic-based communications between parties without revealing the identity of either party. This purpose is elaborated in many different and related, expressly stated goals. Walker, col. 4 lines 17-53. Anonymity is the paramount concern, and the concept permeates every paragraph of the patent, from its title to its claims. Walker's approach is diametrically opposed to, and incompatible with, systems in which the two parties know each other's identities. To quote the *Gordon* court, the primary reference itself teaches away from the proposed modification.

To be specific, the claims of the present application break the anonymity between the candidate and the outside user. Claim 1 expressly states that the candidate identifier "identifies the candidate." The outside user has "received the candidate identifier directly or indirectly from the candidate." Walker's goal of preserving the candidate's anonymity vis-à-vis outside users, and his carefully constructed system for doing just that, are both fundamentally inconsistent with these claim limitations—it is impossible for Walker's invention to maintain the anonymity of any candidate who, directly or indirectly,

communicates information identifying himself to the outside party. By combining Walker with limitation (b) of claim 1 (for which Ballantyne was cited), the Office destroys the function of Walker's invention, rendering it unsuitable for its expressly stated purpose. The same argument is also made against combining Walker with limitation (c) of claim 1 (for which Bisbee was cited). As a matter of law, there is no motivation for combining Walker with Ballantyne and Bisbee in this way. Note that, for the purposes of this argument, the actual disclosures of the secondary references cited against the claim limitations (Ballantyne and Bisbee) are immaterial; it only matters that they are being cited for the purpose of breaking anonymity, which is Walker's primary purpose.

A person having ordinary skill in the art would not have any motivation to use Walker in the combination proposed by the Office. In fact, reason indicates that the skilled person would view Walker as irrelevant to the claimed invention. Why should any person exert the effort to carefully construct Walker's intricate system of hashes and encrypted data to provide anonymity to a person, only to immediately undermine that effort by communicating data identifying that person to the very outside party against whom the anonymity was sought to be maintained? There is no motivation to do so found in the cited art, and the Office does not provide one.

The motivation provided in the Office action for combining Walker with Ballantyne does not address the unsuitability issue. The motivation given by the Office is "to make sure personal background data can be distinctively identified in a secure manner." Office action, p. 4. Yet Walker already provides this functionality in the form of transaction IDs. See Walker, col. 17, lines 4-45. There is no motivation to combine Walker with another reference to obtain this functionality—it's already present in Walker. By contrast, from Walker's perspective, providing a candidate identifier to an outside party is insecure, as doing so directly contradicts Walker's primary goal of preserving anonymity.

A person having ordinary skill in the art would therefore have no motivation to combine Walker with Ballantyne and Bisbee (or with any reference that undermines Walker's delicately constructed anonymity) to reach the limitations of the claims.

Indeed, a skilled person would have a strong disincentive against making such a combination, as doing so would render Walker's system ineffective.

Because there is no motivation to combine these references, the Office has failed to establish a *prima facie* case of obviousness in the combination of Walker, Ballantyne, and Bisbee. For at least this reason, claims 1-16 are not obvious in view of this combination.

Conclusion

For the foregoing reasons, Appellant submits that all claims in the application are allowable over the art of record and a decision of the Board to that effect is respectfully solicited.

Date: January 10, 2011

Respectfully submitted,

/David E. Blau, #60,625/
David E. Blau
Registration No. 60,625
Attorney for Applicant

Sunstein, Kann, Murphy & Timbers LLP
125 Summer Street
Boston, MA 02110-1618
(617) 443-9292

1525B/00116 1387177.3

Appendix I: Claims Appendix

Claim 1: A method of providing access to a candidate's personal background data, wherein the data have been verified, the method comprising:

- a. establishing a data record relating to the candidate's personal background data, in a digital storage medium, the data record having a candidate identifier that identifies the candidate and including
 - (i) a set of components based on information supplied by the candidate, each component being potentially verifiable, and
 - (ii) a corresponding set of query results obtained at a first time, the corresponding set including, with respect to each component, the result of a verification query to a third party;
- b. communicating the candidate identifier to the candidate;
- c. receiving after the first time, over a communication network, the candidate identifier from an outside user wanting verification of the candidate's personal background data, the outside user having received the candidate identifier directly or indirectly from the candidate; and
- d. distributing, to the outside user, over the communication network, in response to receiving the candidate identifier, an electronic document including the data record and an electronic authentication of the contents of the data record, the electronic authentication capable of revealing unauthorized modifications of the contents of the data record.

Claim 2: A method according to claim 1, wherein establishing the data record includes:

- a. from a computer at a first location, separately specifying over a network to a host computer a set of components of the candidate's personal background data, each component being potentially verifiable by contacting a third party;
- b. storing, in a digital storage medium in communication with the host computer, the set of components;
- c. for each component of the set,
identifying a relevant third party and pertinent contact information therefor;
communicating a query to the relevant third party to verify the component,
and obtaining a query result from the query; and
associating the query result with the component and storing the query result in the storage medium.

Claim 3: A method according to claim 2, wherein specifying the set of components includes providing responses via a set of templates, the set of templates having at least one member and being structured to evince the content of the set of components.

Claim 4: A method according to claim 2, wherein specifying the set of components is performed over the Internet.

Claim 5: A method according to claim 4, in which obtaining a query result from the query is performed over the Internet.

Claim 6: A method according to claim 4, wherein specifying the set of components includes specifying the set of components to a World Wide Web server.

Claim 7: A method according to claim 6, in which communicating a query to the relevant third party to verify the component is performed over the Internet.

Claim 8: A method according to claim 7, wherein communicating a query to the relevant third party to verify the component is performed automatically and includes sending the query as E-Mail.

Claim 9: A method according to claim 1, in which communicating the identifier to the candidate is performed over the Internet.

Claim 10: A method according to claim 9, wherein communicating the identifier to the candidate is performed automatically and includes sending the identifier as E-Mail over the Internet.

Claim 11: A method according to claim 1, wherein the electronic document is distributed in the form of an electronic mail message.

Claim 12: A method according to claim 1, wherein the electronic document is distributed in the form of an electronic file.

Claim 13: A method according to claim 1, wherein the electronic authentication is an electronic watermark.

Claim 14: A method according to claim 1, wherein the electronic authentication is an electronic certification.

Claim 15: A method according to claim 1, wherein the set of components includes the candidate's résumé information, and wherein the set of query results includes information verifying the candidate's résumé information.

Claim 16: A system for providing access to a candidate's personal background data, wherein the data have been verified, the system comprising:

(a) a storage arrangement on which is stored a database having a plurality of data records, each data record relating to personal background data of a candidate, each data record having a candidate identifier that identifies the candidate and that is communicated to the candidate, each data record including

(i) a set of components based on information supplied by a candidate, each component being potentially verifiable, and

(ii) a corresponding set of query results obtained at a first time, the corresponding set including, with respect to each component, the result of a verification query to a third party; and

(b) a process, running on a computer in communication with the storage arrangement, for selectively distributing, to an authorized person presenting an identifier received directly or indirectly from the candidate, in response to receiving the identifier after the first time, over a communication network, an electronic document including the candidate's data record and an electronic authentication of the contents of the data record, the electronic authentication capable of revealing unauthorized modifications of the contents of the data record.

Claims 17-56: (canceled)

Appendix II: Evidence Appendix

None.

Appendix III: Related Proceedings Appendix

None.